

U.S. DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON

MICHELE DESOER,

Plaintiff,

vs.

CAPITAL ONE FINANCIAL CORPORATION;
AMAZON WEB SERVICES, INC.,

Defendants.

NO.

CLASS ACTION COMPLAINT

Plaintiff Michele Desoer (“Plaintiff”), by and through her undersigned attorneys, individually and on behalf of all others similarly situated, brings this Class Action Complaint against Defendant Capital One Financial Corporation (“Capital One”) and Amazon Web Services, Inc. (“Amazon”), and makes the following allegations based upon knowledge as to herself and her own acts, and upon information and belief as to all other matters, as follows:

I. INTRODUCTION

1. This is a class action brought by Plaintiff individually and on behalf of all other similarly situated individuals whose personal information, including names, addresses, phone numbers, email addresses, credit histories, income data and other private information (including financial account and social security numbers for certain class members) (hereinafter “Personal

1 Information” or “PI”) was stolen from Defendants’ computer servers beginning on or around
2 March 12, 2019, and lasting until July 17, 2019 (the “Data Breach”).

3 2. On July 29, 2019, the United States Department of Justice indicted a Seattle
4 resident for the Data Breach, alleging that she hacked and exfiltrated personal data for over 100
5 million consumer accounts and applications for credit from Defendants. Capital One also
6 confirmed the data breach publicly, stating on its website that “we determined that an outside
7 individual gained unauthorized access and obtained certain types of personal information about
8 Capital One credit card customers and individuals who had applied for our credit card
9 products.”

10 3. Capital One also proclaimed in the web posting that “safeguarding information
11 is essential to our mission and our role as a financial institution.” Contrary to these statements,
12 however, neither Capital One nor Amazon adequately safeguarded the data entrusted to them
13 and failed to implement even the most basic data security protocols, thereby making the data
14 vulnerable to hackers. Instead, Defendants’ failure to implement and maintain adequate data
15 security measures for their customers’ information, including the PI, directly and proximately
16 caused injury to Plaintiff and the Class defined below.

17 4. As a result of Defendants’ misconduct, the Data Breach compromised the PI of
18 tens of millions of Americans. Victims have had their PI compromised, their privacy violated,
19 are at an increased risk of exposure to fraud and identity theft, have suffered a loss of control
20 over their personal and financial information, and have otherwise been injured. Through this
21 suit, Plaintiff and the Class seek to recover damages caused by Defendants’ breaches of
22 common law duties and violations of state and federal consumer protection statutes. Plaintiff
23 also seeks injunctive and declaratory relief on behalf of herself and similarly-situated Class
24 members.

25
26
27

II. PARTIES

5. Plaintiff Michele Desoer is an adult over the age of eighteen. She is a resident of Calabasas, California. Plaintiff has been a Capital One credit card account holder for the past three to five years and, on information and belief, has had her PI compromised during the Data Breach. As a result of Defendants' failures to adequately safeguard Plaintiff's Personal Information, Plaintiff has been injured.

6. Defendant Capital One is a corporation with a principal executive office in McLean, Virginia. Capital One is a financial services company that provides credit cards and other retail consumer banking products throughout the United States.

7. Defendant Amazon is a corporation with a principal executive office in Seattle, Washington. Defendant Amazon operates a cloud-based computing environment that offers web and server hosting services for third-party companies, including Capital One.

III. JURISDICTION AND VENUE

8. This Court has jurisdiction over the subject matter of this action pursuant to 28 U.S.C. § 1332, as amended by the Class Action Fairness Act of 2005, because the matter in controversy exceeds \$5,000,000, exclusive of interest and costs, and is a class action in which some members of the Class are citizens of different states than Defendants. *See* 28 U.S.C. § 1332(d)(2)(A). This Court has supplemental jurisdiction over the state law claims pursuant to 28 U.S.C. § 1367.

9. This Court has personal jurisdiction over Defendant Capital One because it is authorized to do business in this District and regularly conducts business in this District, and has sufficient minimum contacts with this state and/or sufficiently avails itself of the markets of this state through its promotion, sales, and marketing within this state to render the exercise of jurisdiction by this Court permissible. In addition, the unlawful conduct alleged in this Complaint occurred in, was directed to, and/or emanated in part from this District.

10. This Court has personal jurisdiction over Defendant Amazon because its headquarters are in this District and the unlawful conduct alleged in this Complaint occurred in, was directed to, and/or emanated in part from this District.

11. Venue in this Court is proper pursuant to 28 U.S.C. § 1391 because Defendants are residents of and/or do business in this District, have intentionally availed themselves of the laws and markets within this District by conducting substantial business in this District, and a significant portion of the facts and circumstances giving rise to this Complaint occurred in or emanated from this District and the State of Washington.

IV. FACTUAL ALLEGATIONS

A. Background

12. Defendant Capital One is a financial services company that offers credit cards and other retail banking products directly to consumers throughout the United States. Capital One provides checking and savings accounts, auto loans, and financial services for businesses as well. Capital One is one of the ten largest banks in the United States and is ranked in the upper echelon of the Fortune 500. In the fourth quarter of 2018, Capital One disclosed that 75% of its \$28 billion annual revenue was from its suite of credit card offerings that it heavily markets directly to consumers through television and internet advertising—often with the tagline “What’s in your wallet?”

13. Capital One states on its website that “we take your security very seriously.” In its Privacy Policy for account holders, Capital One represents that “[t]o protect your personal information from unauthorized access and use, we use security measures that comply with federal law. These measures include computer safeguards and secured files and buildings.” Capital One also claims to “protect the confidentiality of Social Security numbers” and that it limits “access to Social Security numbers to employees or others with legitimate business purposes.” In its standard cardmember agreement, Capital One represents and contracts that it

1 “supports information privacy protection” and then incorporates the previously stated privacy
2 policies by reference.

3 14. Capital One’s cardmember agreement also states, “We may report information
4 about your Account to credit bureaus and others. Late payments, missed payments, or other
5 defaults on your Account may be reflected in your credit report. Information we provide may
6 appear on your [] credit reports.”

7 15. Amazon is a subsidiary of Amazon.com, Inc. that provides on demand cloud
8 computing platforms to individuals, companies, and governments. Amazon comprises over 90
9 tech-based services including data storage, security, blockchain, networking, analytics, and
10 developer tools. Companies like Capital One outsource their large amount of consumer data
11 and PI to host on Amazon servers, which are located at “server farms” throughout the world.
12 Amazon advertises on its website that it “offers industry-leading scalability, data availability,
13 security and performance.” Amazon claims that its security is “unmatched” and that business
14 partners can store data with Amazon to “secure it from unauthorized access with encryption
15 features and management tools.”

16 16. Despite these representations and agreements with consumers, Capital One and
17 Amazon failed to disclose that they did not maintain cardmember applications and cardmember
18 PI in compliance with state and federal mandated data security protocols, or even industry
19 standards, in order to prevent the unauthorized access, use, and theft of PI.

20 **B. The Data Breach**

21 17. According to a federal indictment filed on July 29, 2019, a hacker exploited
22 blaring weaknesses in Defendants’ data security protocol over a *four-month* period between
23 March 12, 2019 and July 17, 2019. The U.S. government’s indictment alleges the hacker was
24 able to access servers that Capital One “rented and contracted” from Amazon to exfiltrate and
25 steal “credit card applications and other documents from Capital One.”
26
27

1 18. The government alleges that Capital One received an anonymous tip on July 17,
2 2019 that Capital One's customers' PI had been collected and posted on GitHub, a tech
3 company that provides webhosting and allows users to manage and store files for software
4 development and other uses. Investigations confirmed that the posted data had been collected
5 from Capital One's Amazon server, which was identified by its unique IP address. The
6 government alleges that breaches in Defendants' firewalls allowed the hacker to access folders
7 or buckets of data in Capital One's storage space at Amazon.

8 19. Capital One subsequently determined that more than 700 folders or buckets of
9 consumer data had been accessed and exfiltrated on or about April 21, 2019, although the
10 initial hacking began weeks before and went undetected by Defendants. Further investigation
11 discovered that Defendants were not even using elementary data security protocols for the tens
12 of millions of consumers' account information with encryption or tokenization, falling far
13 below industry standards and best practices espoused by organizations like the National
14 Institute of Standards and Technology (NIST). The elements of data that *were* encrypted were
15 decrypted in the exfiltration, rendering those basic safeguards superfluous.

16 20. Capital One also publicly acknowledged the breach, although it decided not to
17 individually notify all impacted individuals whose PI had been accessed. Instead, Capital One
18 claims it "immediately fixed the issues and began working with federal law enforcement."
19 Capital One also stated that "we believe it is unlikely that the information was used for fraud or
20 disseminated by this individual," although the federal indictment makes clear the hacker made
21 it publicly known on the Internet and social media that she had the data, discussed her
22 possession of it with other individuals, and did not secure it from further use or
23 dissemination—including after it was decrypted. Capital One did not acknowledge that it had
24 not detected the months-long security breach while unsuspecting consumers used and applied
25 for Capital One accounts and that it was only made aware of the breach by a third party.

1 21. Capital One has expressly acknowledged the disclosure of data pertaining to 100
2 million individuals, including:

- 3 • Customer status data such as credit scores, credit limits,
4 balances, payment history, and contact information;
- 5 • Fragments of transaction data from a total of 23 days during
6 2016, 2017 and 2018;
- 7 • About 140,000 Social Security numbers of credit card
8 customers; and
- 9 • About 80,000 linked bank account numbers of secured credit
10 card customers.¹

11 22. Capital One acknowledged that the “largest category of information accessed
12 was information on consumers and small businesses as of the time they applied for one of our
13 credit card products from 2005 through early 2019. This information included data Capital One
14 routinely collects at the time it receives credit card applications, including names, addresses,
15 zip codes/postal codes, phone numbers, email addresses, dates of birth, and self-reported
16 income.” Capital One encouraged its customers to “monitor their credit card accounts for
17 unusual or suspicious activity” and said that they “should be mindful of the possibility of
18 [fraudulent] phishing emails and phone calls due to this incident,” thereby acknowledging that
19 Capital One and Amazon had caused concrete and ongoing harm to consumers as a result of
20 their lack of security protocols. Capital One also proclaimed that the hacker was “the person
21 responsible for this incident,” failing to acknowledge that its weak, rudimentary, and
22 misleading security practices were ultimately to blame.

23 23. After the announcement, Brian Krebs, a prominent data security expert and
24 blogger noted that it was incredible that the breach was known “publicly over several months
25 on social media and other open online platforms.”² He pointed out that the hacker publicly
26 listed “various databases she found by hacking into improperly secured Amazon cloud

27 ¹ <https://www.capitalone.com/facts2019/>.

² <https://krebsonsecurity.com/2019/07/capital-one-data-theft-impacts-106m-people/>.

1 instances.” Mr. Krebs said that “it seems likely that at least some of that data could have been
2 obtained by others who may have followed her activities on different social media platforms.”

3 24. Other commentators have observed that what the hacker “did was only possible
4 because Capital One has misconfigured its Amazon server” and that such misconfigurations are
5 “easily fixed” through industry standard security protocols that Capital One failed to use. The
6 Houston Chronicle reported:

7 Cybersecurity experts said that the mistake is likely attributable to the
8 Capital One information technology employees responsible for installing
9 the firewall to protect access to the company’s data in the cloud. This type
10 of attack could have been prevented by proper diligence and “penetration
11 testing,” which tests the strength of the firewall, according to the Internet
12 Society, a nonprofit internet policy organization.³

13 The same article also criticized Capital One’s investigation and communications with impacted
14 consumers, stating that Capital One “has not been very transparent about the breach” and
15 pointing out that the company’s web post about the breach makes confusing and contradictory
16 statements about whether account numbers were accessed. Moreover, Capital One did not
17 explain why it (or Amazon) did not detect the breach or why it took 12 days to begin notifying
18 impacted customers.

19 25. Defendants’ communications do not comply with their obligation to provide
20 adequate and timely notification of the Data Breach. Capital One is offering impacted
21 customers complimentary credit monitoring and identity protection services, but those services
22 do not sufficiently protect those individuals from the threats data breaches pose and will not be
23 in effect long enough to eliminate all potential damage from the Data Breach.

24 **C. Industry standards, identity theft, and protection of personal information.**

25 26. It is well known that PI, and financial account information in particular, is an
26 invaluable commodity and a frequent target of hackers. Despite this widespread knowledge and
27

³ <https://www.houstonchronicle.com/business/article/The-Capital-One-breach-was-preventable-experts-14268501.php>.

1 industry alerts of other notable data breaches, Defendants failed to take reasonable steps to
2 adequately protect their systems from being breached.

3 27. According to Javelin Strategy & Research, in 2017 alone over 16.7 million
4 individuals were affected by identity theft, causing \$16.8 billion to be stolen.⁴

5 28. Defendants are, and at all relevant times have been, aware that the PI they
6 maintain is highly sensitive and could be used for illegal purposes by third parties. Indeed,
7 Defendants' websites acknowledge that their customers expect adequate security and
8 safeguards of their PI—and Capital One incorporated this acknowledgment into its
9 cardmember agreements.

10 29. Consumers place a high value not only on their PI, but also on the privacy of
11 that data. This is because identity theft causes “significant negative financial impact on
12 victims” as well as severe distress and other strong emotions and physical reactions.⁵

13 30. Consumers are particularly concerned about protecting the privacy of their
14 financial account information and social security numbers, which are the “secret sauce” that is
15 “as good as your DNA to hackers.”⁶ There are long-term consequences to data breach victims
16 whose social security numbers are taken and used by hackers. Even if they know their social
17 security numbers have been accessed, Plaintiff and Class members cannot obtain new numbers
18 unless they become a victim of social security number misuse. Even then, the Social Security
19 Administration has warned that “a new number probably won’t solve all [] problems ... and
20 won’t guarantee ... a fresh start.”⁷

21 _____
22 ⁴ Javelin Strategy & Research, *Identity Fraud Hits All Time High With 16.7 Million U.S.*
23 *Victims in 2017, According to New Javelin Strategy & Research Study* (Feb. 6, 2018),
24 <https://www.javelinstrategy.com/press-release/identity-fraud-hits-all-time-high-167-million-us-victims-2017-according-new-javelin>.

25 ⁵ Identity Theft Resource Center, *Identity Theft: The Aftermath 2017*,
26 https://www.ftc.gov/system/files/documents/public_comments/2017/10/00004-141444.pdf.

27 ⁶ Cameron Huddleston, *How to Protect Your Kids From the Anthem Data Breach*, Kiplinger,
(Feb. 10, 2015), <https://www.kiplinger.com/article/credit/T048-C011-S001-how-to-protect-your-kids-from-the-anthem-data-brea.html>.

⁷ Social Security Admin., *Identity Theft and Your Social Security Number* at 6-7,

1 31. In light of the multiple high-profile data breaches targeting companies like
 2 Target, Neiman Marcus, eBay, Anthem, and Equifax, Defendants are, or reasonably should
 3 have been, aware of the importance of safeguarding their customers' PI, as well as of the
 4 foreseeable consequences of their systems being breached.

5 32. Nonetheless, Defendants failed to upgrade and maintain their data security
 6 systems in a meaningful way so as to prevent the Data Breach. Had Defendants properly
 7 maintained their systems and adequately protected them, they could have prevented the Data
 8 Breach.

9 33. Defendants had a duty to Plaintiff and Class members to properly secure their
 10 PI, encrypt, tokenize, and maintain their PI using industry standard methods, use widely
 11 available technology to defend their systems from invasion, act reasonably to prevent
 12 foreseeable harm to Plaintiff and Class members, and promptly notify Plaintiff and Class
 13 members when Defendants became aware of the potential that their customers' PI may have
 14 been compromised.

15 34. Plaintiff and Class members have suffered injury and damages, including the
 16 increased risk of identity theft and identity fraud, improper disclosure of their PI, the time and
 17 expense necessary to mitigate, remediate, and sort out the increased risk of identity theft and
 18 identity fraud, and a deprivation of the value of their PI.

19 35. Plaintiff and Class members have suffered and will continue to suffer additional
 20 damages based on the opportunity cost and time Plaintiff and Class members are forced to
 21 expend in the future to monitor their financial accounts and credit files as a result of the Data
 22 Breach.

23 V. CLASS ACTION ALLEGATIONS

24 36. Plaintiff brings this class action pursuant to Rule 23 of the Federal Rules of Civil
 25 Procedure on behalf of herself and a Nationwide Class defined as (the "Class"):

26
 27 <https://www.ssa.gov/pubs/EN-05-10064.pdf>.

1 All persons whose Personal Information was compromised in the Data
2 Breach that occurred from at least March 12, 2019 through July 17, 2019.

3 37. Plaintiff further brings this class action pursuant to Rule 23 of the Federal Rules
4 of Civil Procedure on behalf of herself and members of the following class (the “California
5 Subclass”):

6 All persons residing in California whose Personal Information was
7 compromised in the Data Breach that occurred from at least March 12,
8 2019 through July 17, 2019.

9 Excluded from the Class and California Subclass are: (1) any Judge or Magistrate presiding
10 over this action and members of their families; (2) Defendants, Defendants’ subsidiaries,
11 parents, successors, predecessors, and any entity in which Defendants have a controlling
12 interest, and their current or former employees, officers, and directors; (3) counsel for Plaintiff
13 and Defendants; and (4) legal representatives, successors, or assigns of any such excluded
14 persons.

15 38. **Numerosity.** Though the exact number and identities of Class and California
16 Subclass members are unknown at this time, Defendants have confirmed that over 100 million
17 individuals were affected by the Data Breach. Accordingly, the Class and California Subclass
18 are so numerous that joinder of all members is impracticable.

19 39. **Commonality and predominance.** Common questions of law and fact exist as
20 to all Class members. These common questions of law or fact predominate over any questions
21 affecting only individual members of the Class. Common questions include, but are not limited
22 to, the following:

- 23 a. Whether Defendants engaged in wrongful conduct as alleged herein;
- 24 b. Whether Defendants owed a duty to Plaintiff and Class members to
25 adequately protect their Personal Information and to provide timely and accurate notice of the
26 Data Breach to Plaintiff and Class members, and whether Defendants willfully, recklessly, or
27 negligently breached these duties;

1 c. Whether Defendants willfully, recklessly, or negligently failed to
2 maintain and execute reasonable procedures to prevent unauthorized access to their data
3 security networks and to Plaintiff and Class members' Personal Information;

4 d. Whether Defendants' conduct, including their failure to act, resulted in
5 or was the proximate cause of the Data Breach;

6 e. Whether Defendants failed to inform Plaintiff and Class members of the
7 Data Breach in a timely and accurate manner;

8 f. Whether Defendants continue to breach their duties to Plaintiff and Class
9 members;

10 g. Whether Defendants have sufficiently addressed or remedied Plaintiff's
11 and Class members' injuries and have taken adequate preventive and precautionary measures to
12 ensure that Plaintiff and Class members will not experience further harm;

13 h. Whether Defendants engaged in unfair or deceptive practices by failing
14 to disclose that they failed to properly safeguard Plaintiff's and Class members' Personal
15 Information;

16 i. Whether Defendants violated the consumer protection statutes applicable
17 to Plaintiff and members of the Class and California Subclass;

18 j. Whether Plaintiff and Class members suffered damages as a proximate
19 result of Defendants' conduct or failure to act; and

20 k. Whether Plaintiff and Class members are entitled to damages, equitable
21 relief, and other relief.

22 40. **Typicality.** Plaintiff's claims are typical of the claims of the Class and
23 California Subclass she seeks to represent because Plaintiff and all members of the proposed
24 Class and California Subclass have suffered similar injuries as a result of the same practices
25 alleged herein. Plaintiff has no interests adverse to the interests of the other members of the
26 Class and California Subclass.
27

1 41. **Adequacy.** Plaintiff will fairly and adequately protect the interests of the Class
2 and California Subclass, and has retained attorneys experienced in class actions and complex
3 litigation as her counsel.

4 42. **Superiority.** A class action is superior to other available means for the fair and
5 efficient adjudication of this dispute. The injury suffered by each Class member, while
6 meaningful on an individual basis, is not of such magnitude as to make the prosecution of
7 individual actions against Defendants economically feasible. Even if Class members could
8 afford individual litigation, the court system could not. In addition to the burden and expense of
9 managing many actions arising from the Data Breach, individual litigation increases the delay
10 and expense to all parties and the court system presented by the legal and factual issues of the
11 case. By contrast, a class action presents far fewer management difficulties and provides the
12 benefits of single adjudication, economy of scale, and comprehensive supervision by a single
13 court.

14 43. In the alternative, the proposed classes may be certified because:

15 a. the prosecution of separate actions by the individual members of the
16 Class and California Subclass would create a risk of inconsistent adjudications, which could
17 establish incompatible standards of conduct for Defendants;

18 b. the prosecution of individual actions could result in adjudications that as
19 a practical matter would be dispositive of the interests of non-party Class members, or which
20 would substantially impair their ability to protect their interests; and

21 c. Defendants acted or refused to act on grounds generally applicable to the
22 proposed classes, thereby making appropriate final and injunctive relief with respect to
23 members of the Class and California Subclass as a whole.

VI. CLAIMS FOR RELIEF

FIRST CAUSE OF ACTION

WILLFUL VIOLATION OF THE FAIR CREDIT REPORTING ACT

15 U.S.C. §§ 1681 *ET SEQ.*

44. Plaintiff realleges each and every allegation above and incorporates by reference all other paragraphs of this Complaint as if fully set forth herein. Plaintiff asserts this claim on behalf of the Class against Defendant Capital One.

45. One of the fundamental purposes of the FCRA is to protect consumers' privacy. 15 U.S.C. § 1681(a). Protecting consumers' privacy involves adopting reasonable procedures to keep sensitive information confidential. 15 U.S.C. § 1681(b).

46. The FCRA defines a "consumer reporting agency" as any person, which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information or consumers for the purpose of furnishing consumer reports to third parties, and which uses any means or facility of interstate commerce for the purpose of preparing or furnishing consumer reports.

15 U.S.C. § 1681a(f).

47. The FCRA defines a "consumer report" as: any written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected in whole or in part for the purpose of establishing the consumer's eligibility for (A) credit or insurance to be used primarily for personal, family, or household purposes; (B) employment purposes; or (C) any other purpose authorized under 15 U.S.C. § 16881(b).

48. Defendant Capital One regularly assembles consumer information including, among other things, financial and credit information, such as names, dates of birth, account numbers and payment history. Capital One also regularly uses interstate commerce to furnish this type of consumer information to third parties.

1 49. Plaintiff's and Class members' PI constitutes consumer reports under FCRA,
2 because this information bears on, among other things, their creditworthiness, credit standing,
3 credit capacity, character, general reputation, financial information, and personal
4 characteristics, and it is used or collected, in whole or in part, for the purpose of establishing
5 Plaintiff's and Class members' eligibility for credit to be used primarily for personal, family, or
6 household purposes, and for establishing relevant rates.

7 50. FCRA requires the adoption of reasonable procedures with regard to, *inter alia*,
8 the confidentiality and proper utilization of personal information. 15 U.S.C. § 1681(b). FCRA
9 also requires that consumer reporting agencies "maintain reasonable procedures designed to . . .
10 limit the furnishing of consumer reports to the purposes listed under section 1681b of this title."
11 15 U.S.C. § 1681e.

12 51. Capital One's failure to adequately protect and safeguard Plaintiff's and Class
13 members' PI resulted in the disclosure of their personal information to one or more third parties
14 in violation of FCRA because the disclosure was not necessary to carry out the purposes for
15 which Capital One received the information, and it was not permitted by statute, regulation or
16 order. Capital One's violations of FCRA were willful or, at the very least reckless, constituting
17 willfulness.

18 52. As a direct and proximate result of Capital One's willful or reckless failure to
19 adopt and maintain reasonable procedures to limit the furnishing and disclosure of Plaintiff's
20 and Class members' PI to the purposes listed in the statute, Plaintiff's and Class members' PI
21 was disclosed and disseminated to unauthorized third parties. Plaintiff and Class members have
22 suffered injury and harm and will continue to suffer injury and harm because of Capital One's
23 conduct.

24 53. As a further direct or proximate result of Capital One's willful or reckless FCRA
25 violations, as described above, Plaintiff and Class members were (and continue to be) injured
26
27

1 and have suffered (and will continue to suffer) the harms and damages described in this
2 Complaint.

3 54. Accordingly, Plaintiff and Class members are entitled to compensation for their
4 actual damages in an amount to be determined at trial or statutory damages of not less than
5 \$100, and not more than \$1,000, each, as well as attorneys' fees, punitive damages, litigation
6 expenses and costs, pursuant to 15 U.S.C. § 1681n(a). Plaintiff also seeks injunctive relief
7 enjoining the above described wrongful acts and practices of Defendant Capital One and
8 requiring Defendant Capital One to employ and maintain industry accepted standards for data
9 security and privacy.

10 **SECOND CAUSE OF ACTION**
11 **NEGLIGENT VIOLATION OF THE FAIR CREDIT REPORTING ACT**
12 **15 U.S.C. §§ 1681 *ET SEQ.***

13 55. Plaintiff realleges each and every allegation above and incorporates by reference
14 all other paragraphs of this Complaint as if fully set forth herein. Plaintiff asserts this claim on
15 behalf of the Class against Defendant Capital One.

16 56. Defendant Capital One obtained sensitive Personal Information from Plaintiff
17 and Class members in providing financial account and credit services.

18 57. Capital One owed a duty to Plaintiff and Class members to maintain
19 confidentiality and to exercise reasonable care in safeguarding and protecting their Personal
20 Information from being compromised by unauthorized persons. This duty included, *inter alia*,
21 designing, maintaining, and testing its security systems to ensure that Plaintiff's and Class
22 members' Personal Information was adequately protected both in the process of collection and
23 after collection.

24 58. Capital One also owed a duty to Plaintiff and Class members to provide security
25 consistent with industry standards and requirements and to ensure that its computer systems
26 and networks adequately protected Plaintiff's and Class members' Personal Information.
27

1 59. Capital One holds itself out as an expert in compliance, and thus knew or should
2 have known the risks inherent in collecting and storing Personal Information and the critical
3 importance of provide adequate security for that information.

4 60. Capital One's conduct created a foreseeable risk of harm to Plaintiff and Class
5 members. This conduct included but was not limited to Capital One's failure to take reasonable
6 steps and opportunities to prevent and stop the Data Breach. Capital One's conduct also
7 included its decision not to comply with industry standards for the safekeeping and
8 maintenance of Plaintiff's and Class members' Personal Information.

9 61. Capital One knew or should have known that it had inadequate data security
10 practices to safeguard such information, and that hackers would attempt to access the Personal
11 Information in its databases.

12 62. Capital One breached its duties to Plaintiff and Class members by failing to
13 exercise reasonable care and implement adequate security systems, protocols, and practices
14 sufficient to protect Plaintiff's and Class members' Personal Information. Capital One's breach
15 of its duties proximately caused the injuries and damages Plaintiff and Class members have
16 suffered.

17 63. As a direct and proximate result of Capital One's negligent conduct, Plaintiff
18 and Class members suffered injury and are entitled to damages in an amount to be proven at
19 trial. Capital One violated its duties of care with reckless indifference toward the rights of
20 others, such that an award of punitive damages is appropriate.

21 **THIRD CAUSE OF ACTION**
22 **BREACH OF EXPRESS AND IMPLIED CONTRACT**

23 64. Plaintiff realleges each and every allegation above and incorporates by reference
24 all other paragraphs of this Complaint as if fully set forth herein. Plaintiff asserts this claim on
25 behalf of the Class against both Defendants.

26 65. Defendants provide services to Plaintiff and Class members in accordance with
27 the terms of their contracts, cardmember agreements, and privacy policies. Plaintiff and Class

1 members are third-party beneficiaries of any contracts among Defendants. As consideration,
 2 Plaintiff and Class members paid money and/or provided PI to Defendants. Accordingly,
 3 Plaintiff and Class members paid Defendants to properly maintain and store their PI and not
 4 disclose it to unauthorized third parties. Defendants violated their contracts by failing to
 5 employ reasonable and adequate privacy practices and measures, leading to the disclosure of
 6 Plaintiff's and Class members' PI for purposes not required or permitted under the contracts.

7 66. Plaintiff and Class members have been damaged by Defendants' conduct,
 8 including by paying for financial services, privacy, and data security practices they did not
 9 receive, as well as by incurring the harms and injuries arising from the Data Breach now and in
 10 the future.

11 **FOURTH CAUSE OF ACTION** 12 **NEGLIGENCE**

13 67. Plaintiff realleges each and every allegation above and incorporates by reference
 14 all other paragraphs of this Complaint as if fully set forth herein. Plaintiff asserts this claim on
 15 behalf of the Class against all Defendants.

16 68. Plaintiff and Class members entrusted Defendants with highly sensitive and
 17 inherently personal private data subject to confidentiality.

18 69. In requiring, obtaining and storing Plaintiff's and Class members' Personal
 19 Information, Defendants owed a duty of reasonable care in safeguarding this PI.

20 70. Defendants' networks, systems, protocols, policies, procedures and practices
 21 were not adequately designed, implemented, maintained, monitored and tested to ensure that
 22 Plaintiff's and Class member's Personal Information was secured from release, disclosure, and
 23 publication. Once the hacker obtained the PI, she did not prevent it from further use, theft, or
 24 publication.

25 71. Defendants' networks, systems, protocols, policies, procedures and practices
 26 were not reasonable given the sensitivity of the Plaintiff's and Class member's PI.
 27

1 72. Upon learning of the Data Breach, Defendants should have immediately
2 reported the Data Breach to Plaintiff and Class members, credit reporting agencies, the Internal
3 Revenue Service, financial institutions, and all other third parties with a right to know and the
4 ability to mitigate harm to Plaintiff and Class members.

5 73. Despite knowing their networks, systems, protocols, policies, procedures and
6 practices were not adequately designed, implemented, maintained, monitored and tested to
7 ensure that Plaintiff's and Class members' PI were secured from release, disclosure, and
8 publication, Defendants ignored the inadequacies and were unmindful of the risk of release,
9 disclosure, and publication they had created.

10 74. Defendants' behavior evidences a reckless disregard for Plaintiff's and Class
11 members' rights. Defendants' negligence is directly linked to Plaintiff's and Class members'
12 injuries.

13 75. As a result of Defendants' reckless disregard for Plaintiff's and Class members'
14 rights by failing to secure their Personal Information despite knowing their networks, systems,
15 protocols, policies, procedures, and practices were not adequately designed, implemented,
16 maintained, monitored, and tested, Plaintiff and Class members suffered injury, including but
17 not limited to the impermissible release, disclosure, and publication—both directly and
18 indirectly by Defendants as well as unauthorized parties—of their Personal Information as well
19 as exposure to a heightened, imminent risk of fraud, identity theft, financial and other harm.
20 Plaintiff and Class members must monitor their financial accounts and credit histories more
21 closely and frequently. Plaintiff and Class members have also incurred and will continue to
22 incur costs for the time and expense necessary to obtain credit reports, credit freezes, credit
23 monitoring services, and other protective measures to deter or detect identity theft. The
24 impermissible release, disclosure, and publication of Plaintiff's and Class members' PI has also
25 diminished the value of their PI.

77. Plaintiff and Class members are entitled to damages in an amount to be proven at trial.

FIFTH CAUSE OF ACTION
NEGLIGENT MISREPRESENTATION

78. Plaintiff realleges each and every allegation above and incorporates by reference all other paragraphs of this Complaint as if fully set forth herein. Plaintiff asserts this claim on behalf of the Class against both Defendants.

79. Defendants negligently represented that they would maintain adequate data privacy and security practices and procedures to safeguard Plaintiff and Class members' Personal Information from impermissible release, disclosure, and publication.

80. Prior to making these representations, Defendants knew or should have known that their networks, systems, protocols, policies, procedures and practices were not adequately designed, implemented, maintained, monitored and tested to ensure that Plaintiff's and Class members' PI were adequately secured from release, disclosure, and publication.

81. Plaintiff and other reasonable consumers, including Class members, reasonably relied on Defendants' representations and, in reliance thereon, engaged, used, and purchased Defendants' services.

82. Plaintiff's and Class members' reliance was reasonable and justified in that Defendants appeared to be, and represented themselves to be, reputable businesses that sold financial and technological services, and touted their data privacy and security measures.

83. Plaintiff and Class members would not have entrusted their Personal Information or otherwise purchased or used Defendants' services had they known that

1 Defendants' data privacy and security practices and procedures were inadequate and risked
2 disclosure of Plaintiff's and Class members' Personal Information.

3 84. As a direct and proximate result of these representations, Plaintiff and Class
4 members suffered injury, including but not limited to the release, disclosure, and publication of
5 their Personal Information as well as exposure to a heightened, imminent risk of fraud, identity
6 theft, financial, and other harm. Plaintiff and Class members must monitor their financial
7 accounts and credit histories more closely and frequently. Plaintiff and Class members also
8 have incurred, and will continue to incur, costs for the time and expense of obtaining credit
9 reports, credit freezes, credit monitoring services, and other protective measures to deter or
10 detect identity theft. The impermissible release, disclosure, and publication of Plaintiff's and
11 Class members' PI has also diminished the value of their PI.

12 85. Plaintiff and Class members are entitled to damages to be determined at trial.

13 **SIXTH CAUSE OF ACTION**
14 **BREACH OF FIDUCIARY DUTY**

15 86. Plaintiff realleges each and every allegation above and incorporates by reference
16 all other paragraphs of this Complaint as if fully set forth herein. Plaintiff asserts this claim on
17 behalf of the Class against both Defendants.

18 87. Defendants owed a fiduciary duty to Plaintiff and the Class as guardians of their
19 Personal Information to (a) protect Plaintiff's and Class members' Personal Information; and
20 (b) timely notify Plaintiff and Class members of the Data Breach.

21 88. Defendants breached their fiduciary duty to Plaintiff and the Class by (a) failing
22 to adequately secure Plaintiff's and Class members' Personal Information from impermissible
23 release, disclosure, and publication; (b) failing to take adequate actions to prevent release,
24 disclosure, and publication of Plaintiff's and Class members' Personal Information, acting in a
25 manner that would be highly offensive to a reasonable person; (c) failing to take adequate
26 action to prevent release, disclosure, and publication of Plaintiff's and Class members' Personal
27

1 Information to unauthorized parties without the informed and clear consent of Plaintiff and the
 2 Class; and (d) belatedly and inadequately notifying Plaintiff and the Class of the Data Breach.

3 89. As a direct and proximate cause of Defendants' conduct, Plaintiff and Class
 4 members suffered an injury in fact and are entitled to relief, including restitution, declaratory
 5 relief, and a permanent injunction enjoining Defendants from further conduct that puts
 6 Plaintiff's and Class members' Personal Information at risk.

7 **SEVENTH CAUSE OF ACTION**
 8 **DECLARATORY JUDGMENT**

9 90. Plaintiff realleges each and every allegation above and incorporates by reference
 10 all other paragraphs of this Complaint as if fully set forth herein. Plaintiff asserts this claim on
 11 behalf of the Class against both Defendants.

12 91. Plaintiff and the Class have stated claims against Defendants for negligence,
 13 gross negligence, negligent misrepresentation, breach of implied contract, and breach of
 14 fiduciary duty.

15 92. Defendants failed to fulfill their obligations to provide adequate and reasonable
 16 data security measures for the Personal Information of Plaintiff and the Class, as evidenced by
 17 the Data Breach.

18 93. As a result of the Data Breach, Defendants' systems are more vulnerable to
 19 access by unauthorized parties and require more stringent measures to be taken to safeguard the
 20 Plaintiff's and Class members' Personal Information going forward.

21 94. An actual controversy has arisen in the wake of the Data Breach regarding
 22 Defendants' current obligations to provide data security measures that will adequately protect
 23 Plaintiff's and Class members' Personal Information.

24 95. Plaintiff seeks a declaration that Defendants must implement specific additional,
 25 prudent, industry-standard data security practices to provide reasonable protection and security
 26 to Plaintiff and Class members' Personal Information. Specifically, Plaintiff and the Class seek
 27 a declaration that Defendants' existing security measures do not comply with their obligations,

1 and that Defendants must implement and maintain reasonable data security measures on behalf
2 of Plaintiff and the Class to comply with their data security obligations.

3 **EIGHTH CAUSE OF ACTION**

4 **VIOLATION OF THE WASHINGTON CONSUMER PROTECTION ACT—**
5 **DECEPTIVE BUSINESS PRACTICES,**
6 **RCW 19.86, *ET SEQ.***

7 96. Plaintiff realleges each and every allegation above and incorporates by reference
8 all other paragraphs of this Complaint as if fully set forth herein. Plaintiff asserts this claim on
9 behalf of the Class against both Defendants.

10 97. Defendants are “persons” within the meaning of the Washington Consumer
11 Protection Act, RCW 19.86.010(1), and conduct “trade” and “commerce” within the meaning
12 of the Washington Consumer Protection Act, RCW § 19.86.010(2).

13 98. The conduct alleged in this Complaint is deceptive within the meaning of the
14 Washington Consumer Protection Act, RCW 19.86.010, *et seq.* Defendants did not disclose
15 their failure to take reasonable step to protect the security of Plaintiff’s and Class members’
16 Personal Information. Defendants also failed to timely and adequately disclose the Data
17 Breach.

18 99. Defendants’ omissions had the capacity to deceive a substantial portion of the
19 public and have impacted the public interest and injured Plaintiff and the Class.

20 100. Defendants’ omissions are material to reasonable consumers like Plaintiff and
21 Class members because reasonable consumers place a high value not only on their Personal
22 Information, but also on the privacy of that data.

23 101. Defendants’ deceptive acts or practices have repeatedly occurred in trade or
24 commerce within the meaning of the CPA, RCW 19.86.010(2) and RCW 19.86.020.

25 102. The acts complained of herein are ongoing or have a substantial likelihood of
26 being repeated.

103. Defendants' deceptive acts or practices impact the public interest because they injured Plaintiff and Class members and have the capacity to injure millions more.

104. As a result of Defendants' deceptive conduct, Plaintiff and the Class are entitled to recover damages from Defendants in an amount to be proven at trial. Furthermore, pursuant to RCW § 19.86.090, Plaintiff and the Class are entitled to trebling of their proven damages.

105. Plaintiff and the Class are also entitled to an award of attorneys' fees pursuant to RCW § 19.86.090.

106. Plaintiff and the Class are entitled to an order, *inter alia*, declaring Defendants' conduct unlawful, and permanently enjoining Defendants from further violations of the Consumer Protection Act.

NINTH CAUSE OF ACTION
VIOLATION OF THE WASHINGTON CONSUMER PROTECTION ACT—
UNFAIR BUSINESS PRACTICES,
RCW 19.86, *ET SEQ.*

107. Plaintiff realleges each and every allegation above and incorporates by reference all other paragraphs of this Complaint as if fully set forth herein. Plaintiff asserts this claim on behalf of the Class against both Defendants.

108. Defendants are "persons" within the meaning of the Washington Consumer Protection Act, RCW 19.86.010(1), and conduct "trade" and "commerce" within the meaning of the Washington Consumer Protection Act, RCW § 19.86.010(2).

109. The conduct described in this Complaint is unfair within the meaning of the Washington Consumer Protection Act, RCW 19.86.010, *et seq.* Defendants knew and should have known that Plaintiff's and Class members' Personal Information is highly sensitive and could be used for illegal purposes by third parties. Nonetheless, Defendants did not adequately safeguard the data entrusted to them and failed to implement even the most basic data security protocols, making the data vulnerable to hackers. Defendants also failed to timely and adequately disclose the Data Breach to consumers.

110. Defendants' acts or practices are unfair because they (1) caused injury to Plaintiff and Class members; (2) are not outweighed by any countervailing benefits to consumers or competitors; and (3) are not reasonably avoidable by consumers.

111. Defendants' acts or practices are also unfair because they are immoral, unethical, oppressive, or unscrupulous.

112. Defendants' unfair acts or practices have repeatedly occurred in trade or commerce within the meaning of the CPA, RCW 19.86.010(2) and RCW 19.86.020.

113. The acts complained of herein are ongoing or have a substantial likelihood of being repeated.

114. Defendants' unfair acts or practices impact the public interest because they injured Plaintiff and Class members and have the capacity to injure millions more.

115. As a direct and proximate result of Defendants' unfair acts or practices, Plaintiff and Class members suffered injury.

116. Plaintiff and Class members are therefore entitled to legal relief against Defendant, including recovery of actual damages, treble damages, attorneys' fees, costs of suit, and such further relief as the Court may deem proper.

117. Plaintiff and Class members are also entitled to injunctive relief in the form of an order prohibiting Defendants from engaging in the alleged misconduct and such other equitable relief as the Court deems appropriate, including but not limited to, disgorgement, for the benefit of Class members, of all or part of the ill-gotten profits received from Defendants' unlawful practices.

TENTH CAUSE OF ACTION
VIOLATION OF THE WASHINGTON DATA BREACH LAW,
RCW 19.255, *ET SEQ.*

118. Plaintiff realleges each and every allegation above and incorporates by reference all other paragraphs of this Complaint as if fully set forth herein. Plaintiff asserts this claim on behalf of the Class against both Defendants.

119. The Washington Data Breach Law provides that “[a]ny person or business that maintains computerized data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.” RCW § 19.255.010(2).

120. The Data Breach resulted in the “unauthorized acquisition of computerized data that compromise[d] the security, confidentiality, [and] integrity of personal information maintained by” Defendants, who therefore experienced a “breach of the security of [their] system[s],” as defined by RCW § 19.255.010(4).

121. Defendants failed to disclose that the Personal Information of over 100 million customers had been compromised immediately upon discovery of the Data Breach, and in doing so unreasonably delayed informing Plaintiff and the Class about the Data Breach when Defendants knew or should have known that the Data Breach had occurred.

122. As a result of the violation of RCW § 19.255.010(2), Plaintiff and Class members have been damaged and, pursuant to RCW § 19.255.010(13), are entitled to recover damages and an injunction, enjoining Defendants from their unlawful practices.

ELEVENTH CAUSE OF ACTION
VIOLATION OF CALIFORNIA CUSTOMER RECORDS ACT,
CALIFORNIA CIVIL CODE §§ 1798.80, *ET SEQ.*

123. Plaintiff realleges each and every allegation above and incorporates by reference all other paragraphs of this Complaint as if fully set forth herein. Plaintiff asserts this claim on behalf of the California Subclass against both Defendants.

124. Defendants are “business[es]” within the meaning of California Civil Code § 1798.80(a).

125. Plaintiff and each member of the California Subclass are “individuals” within the meaning of California Civil Code § 1798.80(c).

1 126. California Civil Code § 1798.81.5 provides that a business that owns, licenses,
2 or maintains personal information about a California resident shall implement and maintain
3 reasonable security procedures and practices appropriate to the nature of the information, to
4 protect the personal information from unauthorized access, destruction, use, modification, or
5 disclosure.

6 127. Plaintiff and California Subclass members provided Personal Information to
7 Defendants that constitutes computerized data and includes Personal Information that is owned,
8 licensed, or maintained by Defendants.

9 128. Defendants failed to implement and maintain reasonable security procedures and
10 practices appropriate to the nature of the information, to protect the personal information from
11 unauthorized access, destruction, use, modification, or disclosure.

12 129. Defendants' failure to have reasonable measures in place to secure the Personal
13 Information was grossly negligent.

14 130. Defendants violated the Customer Records Act by failing to notify California
15 residents in the most expedient time possible and without unreasonable delay. Defendants
16 expressly learned of the Data Breach as early as July 17, 2019, but reasonably should have
17 discovered it much earlier. Upon learning of the Data Breach, Defendants failed to disseminate
18 the required notification to Plaintiff and the other California Subclass members until around
19 July 29, 2019.

20 131. Defendants' notification of the Data Breach was insufficient, misleading, and
21 not compliant with the law.

22 132. California law gives the protection of its citizens' privacy the highest priority.
23 Article 1, Section 1 of the California Constitution states that "All people are by nature free and
24 independent and have inalienable rights. Among these are enjoying and defending life and
25 liberty, acquiring, possessing and protecting property, and pursuing and obtaining safety,
26 happiness and privacy."
27

133. California's common law and statutory scheme also recognizes and protects California residents' right of privacy. For example, California Civil Code § 1798.81.5(a) states: "It is the intent of the Legislature to ensure that personal information about California residents is protected. To that end, the purpose of this section is to encourage businesses that own or license personal information about Californians to provide reasonable security for that information."

134. California citizens' rights to privacy have been compromised and infringed by the Defendants' acts and omissions.

135. Under California Civil Code § 1798.84, any customer injured by a violation of this title may institute a civil action to recover damages. Any business that violates, proposes to violate, or has violated this title may be enjoined.

136. As a result of Defendants' violations of the Customer Records Act and the Data Breach, Plaintiff and the other California Subclass members were injured and incurred actual harm and damages. Plaintiff and the other Subclass members have suffered actual damages, including identity theft, improper disclosure of their Personal Information, lost value of their Personal Information, lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risk of identity theft that resulted and continues to face them.

TWELFTH CAUSE OF ACTION
VIOLATION OF THE UNFAIR COMPETITION ACT,
BUSINESS & PROFESSIONS CODE § 17200, *ET SEQ.*

137. Plaintiff realleges each and every allegation above and incorporates by reference all other paragraphs of this Complaint as if fully set forth herein. Plaintiff asserts this claim on behalf of the California Subclass against both Defendants.

138. California Business & Professions Code § 17200, *et seq.* (the "UCL") provides that unfair practices include, but are not limited to, "any unlawful, unfair or fraudulent business act[s] or practice[s]."

1 139. Defendants engaged in activities that constitute unlawful, unfair and fraudulent
2 business practices prohibited by the UCL.

3 140. Defendants knew or should have known that their failure to implement and
4 maintain reasonable security procedures and practices to protect Plaintiff's and the other
5 California Subclass members' Personal Information was unlawful, unfair, and fraudulent.
6 Defendants willfully ignored the clear and present risk of a security breach of their systems and
7 failed to implement and maintain reasonable security measures to prevent, detect, and mitigate
8 the Data Breach. Defendants benefitted from not taking preventative measures and
9 implementing adequate security measures that would have prevented, detected, and mitigated
10 the Data Breach.

11 141. Defendants' conduct is unlawful because it violates FCRA, the California
12 Consumers Legal Remedies Act, and constitutes negligence and negligent misrepresentation.

13 142. Defendants' conduct was unfair because it violates established public policy
14 established by FCRA and California law governing the security and privacy of consumers'
15 personal information. Defendants' conduct is also immoral, unethical, oppressive or
16 unscrupulous and causes injury to consumers that outweighs its benefits. Any benefit to
17 consumers of Defendants' services is outweighed by the harm to consumers of the disclosure of
18 their Personal Information. Consumers could not have avoided this harm themselves.

19 143. Defendants' conduct is fraudulent because they made representations and
20 omissions on their websites about the strength and adequacy of their security measures when in
21 fact their systems were vulnerable to unauthorized access. Defendants' security measures were
22 also unable to detect suspicious and unauthorized activity for a period of at least one month,
23 and perhaps longer.

24 144. Plaintiff and the other California Subclass members have suffered actual
25 damages including identity theft, improper disclosure of their Personal Information, lost value
26
27

1 of their Personal Information, lost time and money incurred to mitigate and remediate the
2 effects of the Data Breach.

3 145. Plaintiff's and the other California Subclass members' injuries were proximately
4 caused by Defendants' violations of the UCL. Defendants acted with reckless indifference
5 toward the rights of others, such that an award of punitive damages is warranted.

6 146. Plaintiff and the other California Subclass members are also entitled to
7 injunctive relief in the form of deletion and destruction of data, greater security practices and
8 protocols, and training and compliance with industry standards governing data security.

9 **THIRTEENTH CAUSE OF ACTION**
10 **VIOLATION OF THE CALIFORNIA CONSUMERS LEGAL REMEDIES**
11 **ACT, CAL. CIV. CODE §§ 1750, *ET SEQ.***

12 147. Plaintiff realleges each and every allegation above and incorporates by reference
13 all other paragraphs of this Complaint as if fully set forth herein. Plaintiff asserts this claim on
14 behalf of the California Subclass against both Defendants.

15 148. Defendants engaged in following prohibited conduct in violation of the
16 California Consumer Legal Remedies Act, Cal. Civ. Code § 1770, among others:

- 17 a. Misrepresenting the source, sponsorship, approval, or certification of
18 goods or services;
- 19 b. Representing that goods or services have characteristics that they do not
20 have;
- 21 c. Representing that goods or services are of a particular standard, quality,
22 or grade when they are not;
- 23 d. Advertising goods or services with intent not to sell them as advertised;
24 and
- 25 e. Representing that the subject of a transaction has been supplied in
26 accordance with a previous representation when it has not.

149. Defendants' representations and omissions were material and likely to mislead a reasonable consumer about the quality of Defendants' data security and ability to protect Personal Information in the provision of financial services.

150. Plaintiff and the other California Subclass members have suffered actual damages, including identity theft, improper disclosure of their Personal Information, lost value of their Personal Information, lost time and money incurred to mitigate and remediate the effects of the Data Breach. Plaintiff is providing the statutory notice required under the CLRA and will amend this claim to assert a request for damages at the end of the statutory waiting period if Defendants do not take corrective action.

VII. PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and on behalf of the Class and California Subclass, prays for relief as follows:

- A. For an order certifying the Class and California Subclass and appointing Plaintiff as class representative;
- B. Awarding monetary and actual damages and/or restitution, as appropriate;
- C. Awarding punitive damages, as appropriate;
- D. Awarding declaratory and injunctive relief as permitted by law or equity to ensure that the Class and California Subclass have an effective remedy, including enjoining Defendants from continuing their unlawful practices;
- E. Prejudgment interest to the extent allowed by the law;
- F. Awarding all costs, including expert fees and attorneys' fees, expenses and costs of prosecuting this action; and
- G. Such other and further relief as the Court may deem just and proper.

VIII. JURY TRIAL DEMAND

Plaintiff, individually and on behalf of all others similarly situated, demands a trial by jury on all issues so triable.

1 RESPECTFULLY SUBMITTED AND DATED this 5th day of August, 2019.

2 TERRELL MARSHALL LAW GROUP PLLC

3 By: /s/ Beth E. Terrell, WSBA #26759
4 Beth E. Terrell, WSBA #26759
5 Email: bterrell@terrellmarshall.com

6 By: /s/ Amanda M. Steiner, WSBA #29147
7 Amanda M. Steiner, WSBA #29147
8 Email: asteiner@terrellmarshall.com

9 By: /s/ Jennifer Rust Murray, WSBA #36983
10 Jennifer Rust Murray, WSBA #36983
11 jmurray@terrellmarshall.com
12 936 North 34th Street, Suite 300
13 Seattle, Washington 98103-8869
14 Telephone: (206) 816-6603

15 Laurence D. King*
16 lking@kaplanfox.com
17 Matthew George*
18 mgeorge@kaplanfox.com
19 Mario M. Choi*
20 mchoi@kaplanfox.com
21 KAPLAN FOX & KILSHEIMER LLP
22 350 Sansome Street, Suite 400
23 San Francisco, California 94104
24 Telephone: (415) 772-4700
25 Facsimile: (415) 772-4707

26 Marc A. Wites*
27 mwites@witeslaw.com
WITES LAW FIRM
4400 North Federal Highway
Lighthouse Point, Florida 33064
Telephone: (954) 933-4400

*Pro Hac Vice Application Forthcoming

*Attorneys for Plaintiff and the proposed Class and
Subclass*